



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/900,494	07/06/2001	Michael Freed	NEXSI-01112US0	4136

28863 7590 04/28/2005
SHUMAKER & SIEFFERT, P. A.
8425 SEASONS PARKWAY
SUITE 105
ST. PAUL, MN 55125

EXAMINER

MOORTHY, ARAVIND K

ART UNIT PAPER NUMBER

2131

DATE MAILED: 04/28/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/900,494	Applicant(s) FREED ET AL.	
	Examiner Aravind K. Moorthy	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 08 April 2005.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-28 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-28 is/are rejected.
- 7) ☐ Claim(s) _____ is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 06 July 2001 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|---|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152) |
| 3) <input checked="" type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

Te

DETAILED ACTION

1. This is in response to the amendment filed on 18 January 2005.
2. Claims 1-28 are pending in the application.
3. Claims 1-28 have been rejected.

Response to Amendment

4. The examiner approves the amendment to claims 1, 5 and 11. The misspellings in the claims have been corrected.

Response to Arguments

5. Applicant's arguments with respect to claims 1-21 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

6. Claims 1-7 and 22 are rejected under 35 U.S.C. 102(e) as being anticipated by Devine et al U.S. Patent No. 6,598,167 B2.

As to claim 1, Devine et al discloses a load balancing acceleration device, comprising:

a processor, memory and communications interface [column 6, lines 33-38];

a TCP communications manager capable of interacting with a plurality of client devices and server devices simultaneously via the communications interface [column 8 line 61 to column 9 line 19];

a secure communications manager to negotiate a secure communication session with one of the client devices [column 8 line 61 to column 9 line 19];

an encryption and decryption engine instructing the processor to decrypt data received via the secure communications session and direct the decrypted data it to one of said server devices via a second communication session [column 23, lines 20-50]; and

a load balancing engine associating each of said client devices with a respective one of said servers devices based on calculated processing loads of each said server devices [column 23, lines 20-50].

As to claim 2, Devine et al discloses that the TCP communications manager provides an IP address of an enterprise to said secure communications manager, and each of said plurality of server devices is associated with the enterprise [column 8 line 61 to column 9 line 19].

As to claim 3, Devine et al discloses that the secure communications manager negotiates a secure communication session with each of said plurality of client devices over an open network [column 23, lines 20-50].

As to claim 4, Devine et al discloses that the TCP communications manager negotiates a separate, open communications session with one of the plurality of server devices associated with the enterprise for each secure communications session negotiated with the client devices based on the associations of said client devices to said server devices said load balancing engines [column 8 line 61 to column 9 line 19].

As to claim 5, Devine et al discloses that the encryption and decryption engine decrypts the data on a packet level by decrypting packet data received on the communications interface via the secure communications session to extract a secure record [column 23, lines 20-50]. Devine et al discloses decrypting application data from the secure record in the packet data [column 23, lines 20-50]. Devine et al discloses outputting the decrypted application data from the secure record to the one of said server devices via the second communication session without processing the application data with an application layer of a TCP/IP stack [column 8 line 61 to column 9 line 19].

As to claim 6, Devine et al discloses that the load-balancing engine selects the second communication session [column 12 line 66 to column 13 line 25].

As to claim 7, Devine et al discloses that the TCP communications manager responds to TCP communications negotiations directly for an enterprise [column 8 line 61 to column 9 line 19].

As to claim 22, Devine et al discloses that the device comprises a network router [column 22, lines 47-65].

7. Claims 1-7 and 22 are rejected under 35 U.S.C. 102(e) as being anticipated by Huppenthal U.S. Patent No. 6,434,687 B1.

As to claim 12, Huppenthal discloses a method for performing acceleration of data communications between a plurality of customer devices attempting to communicate with an enterprise having a plurality of servers, comprising:

providing an intermediate acceleration device enabled for secure communication with the customer devices, wherein the acceleration device has an IP address associated with the enterprise [column 4, lines 26-55];

receiving with the acceleration device communications directed to the enterprise in a secure protocol from one of the customer devices [column 5, lines 37-63];

decrypting data packets of the secure protocol with the acceleration device to provide decrypted packet data [column 6, lines 38-55];

selecting with the acceleration device at least one of the plurality of servers in the enterprise based on a load calculation including processing sessions of other servers in the enterprise and associating the selected server with a communications session from the one of the clients [column 7, lines 1-25]; and

forwarding the decrypted packet data from the acceleration device to the selected server of the enterprise [column 7, lines 1-25].

As to claim 13, Huppenthal discloses the steps of receiving application data from the selected server of the enterprise, encrypting the application data received from the selected server, and forwarding encrypted application data to the customer device [column 7, lines 1-25].

As to claim 14, Huppenthal discloses that the step of receiving communications directed to the enterprise includes receiving with the device communications having a destination IP address of the enterprise [column 8, lines 7-19].

As to claim 15, Huppenthal discloses the step of negotiating the secure protocol session with the customer device by responding as the enterprise to the customer device [column 7, lines 1-25]s.

As to claim 17, Huppenthal discloses that the step of forwarding comprises:

establishing an open communication session from the acceleration device to the selected server [column 7, lines 1-25], and

mapping the decrypted packet data to the open communication session established with the selected server [column 7, lines 1-25].

As to claim 18, Huppenthal discloses that the open communication session is established via a secure network [column 7, lines 1-25].

As to claim 19, Huppenthal discloses that the step of receiving comprises:

receiving encrypted data having a length greater than a TCP segment carrying said data [column 8, lines 47-67]; and

wherein said step of decrypting comprises:

buffering the encrypted data in a memory buffer in the acceleration device, the buffer having a length equivalent to the block cipher size necessary to perform the cipher [column 8, lines 47-67]; and
decrypting the buffered segment of the received encrypted data to provide decrypted application data [column 7, lines 1-25].

As to claim 20, Huppenthal discloses the step of authenticating the data on receipt of a final TCP segment on a packet level without processing the application data with an application layer of a TCP/IP stack [column 9, lines 43-67].

As to claim 21, Huppenthal discloses the step of generating an alert if said step of authenticating results in a failure [column 14, lines 40-58].

As to claim 23, Huppenthal discloses decrypting data packets comprises decrypting the data packets at a packet level of a TCP/IP stack [column 9, lines 43-67].

As to claim 24, Huppenthal discloses that decrypting data packets comprises:

decrypting the data packets to extract a secure record [column 7, lines 1-25],
decrypting application data from the secure record [column 7, lines 1-25],
and
authenticating the application data without processing the application data with an application layer of a TCP/IP stack [column 7, lines 1-25].

8. Claims 25-28 are rejected under 35 U.S.C. 102(e) as being anticipated by Baskey et al U.S. Patent No. 6,732,269 B1.

As to claim 25, Baskey et al discloses a system comprising:

a client device [column 5, lines 17-57];

a plurality of server devices [column 5, lines 17-57]; and

an intermediate device coupled between the client devices and the server devices [column 5, lines 17-57],

wherein the intermediate device intercepts a request from the client device for a secure communication session [column 5 line 58 to column 6 line 16], and

wherein, in response to the request, the intermediate device establishes a secure communication session with the client device, selects one of the server devices based on resource loading experienced by the server devices, and establishes a non-secure communication session with the selected server device [column 5 line 58 to column 6 line 16].

As to claim 26, Baskey et al discloses that the intermediate device receives encrypted data from the client device via the secure communication session, decrypts the data and forwards the decrypted data to the selected server device via the non-secure communication session [column 8 line 51 to column 9 line 19].

As to claim 27, Baskey et al discloses that the intermediate device receives unencrypted data from the selected server device via the non-secure communication session, encrypts the data and forwards the encrypted data to the client device via the secure communication session [column 8 line 51 to column 9 line 19].

As to claim 28, Baskey et al discloses that the intermediate device comprises a network router [column 5, lines 17-57].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

9. Claims 8-11 is rejected under 35 U.S.C. 103(a) as being unpatentable over Devine et al U.S. Patent No. 6,598,167 B1 as applied to claim 1 above, and further in view of Gelman et al U.S. Patent No. 6,415,329 B1.

As to claims 8 and 11, Devine et al does not teach that the secure communications manager changes a destination IP address for each packet to a server IP address for each session.

Gelman et al teaches a secure communications manager that changes a destination IP address for each packet to a server IP address for each session [column 10, lines 9-21].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Devine et al so that the proxy server would have changed the destination IP address for each packet to one of the server IP addresses for each session.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Devine et al by the teaching of Gelman et al because the detrimental effects of latency and errors on TCP are avoided and link utilization is greatly increased. TCP/IP headers are replaced with a much shorter WLP header, leaving more

bandwidth for data. In addition, TCP/IP data may be compressed so that fewer bytes need to be sent over the wireless segment, thus improving data transfer times. Encryption may also be used to protect data from eavesdropping. Finally, the system may be implemented without making any changes to the TCP/IP code on the gateway. No changes of any kind are required to the end users [column 5, lines 54-67].

As to claim 9, Devine teaches that the TCP communications manager maintains TCP communication sessions with the server devices, and wherein the secure communications manager engine negotiates a secure communication session for each TCP communications session [column 23, lines 20-50].

As to claim 10, Devine teaches that the secure communications manager responds to all secure communications with each client device [column 23, lines 20-50].

10. Claim 16 is rejected under 35 U.S.C. 103(a) as being unpatentable over Huppenthal U.S. Patent No. 6,434,687 B1 as applied to claim 12 above, and further in view of Gelman et al U.S. Patent No. 6,415,329 B1.

As to claim 16, Lincke et al does not teach that the step of forwarding comprises modifying the destination IP address of data packets from the enterprise IP to an IP for the selected server.

Gelman et al teaches a secure communications manager that changes a destination IP address for each packet to a selected server IP address for each session [column 10, lines 9-21].

Therefore, it would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Lincke et al so that the proxy server would have

Art Unit: 2131

changed the destination IP address for each packet to one of the server IP addresses for each session.

It would have been obvious to a person having ordinary skill in the art at the time the invention was made to have modified Lincke et al by the teaching of Gelman et al because the detrimental effects of latency and errors on TCP are avoided and link utilization is greatly increased. TCP/IP headers are replaced with a much shorter WLP header, leaving more bandwidth for data. In addition, TCP/IP data may be compressed so that fewer bytes need to be sent over the wireless segment, thus improving data transfer times. Encryption may also be used to protect data from eavesdropping. Finally, the system may be implemented without making any changes to the TCP/IP code on the gateway. No changes of any kind are required to the end users [column 5, lines 54-67].

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event,

Art Unit: 2131

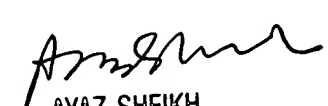
however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Aravind K. Moorthy whose telephone number is 571-272-3793. The examiner can normally be reached on Monday-Friday, 8:00-5:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Aravind K Moorthy
April 21, 2005



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100